



## Testimony

Before the Subcommittee on Oversight and  
Investigations, Committee on Energy and Commerce,  
House of Representatives

---

For Release on Delivery  
Expected at 9:00 a.m. EDT  
Tuesday, July 9, 2002

# CRITICAL INFRASTRUCTURE PROTECTION

## Significant Homeland Security Challenges Need to Be Addressed

Statement of Robert F. Dacey  
Director, Information Security Issues



## Report Documentation Page

<b>Report Date</b> 00JUL2002	<b>Report Type</b> N/A	<b>Dates Covered (from... to)</b> -
<b>Title and Subtitle</b> CRITICAL INFRASTRUCTURE PROTECTION: Significant Homeland Security Challenges Need to Be Addressed		<b>Contract Number</b>
		<b>Grant Number</b>
		<b>Program Element Number</b>
<b>Author(s)</b>		<b>Project Number</b>
		<b>Task Number</b>
		<b>Work Unit Number</b>
<b>Performing Organization Name(s) and Address(es)</b> U.S. General Accounting Office 441 G Street NW, Room LM Washington, DC 20548		<b>Performing Organization Report Number</b> GAO-02-918t
<b>Sponsoring/Monitoring Agency Name(s) and Address(es)</b>		<b>Sponsor/Monitor's Acronym(s)</b>
		<b>Sponsor/Monitor's Report Number(s)</b>
<b>Distribution/Availability Statement</b> Approved for public release, distribution unlimited		
<b>Supplementary Notes</b>		
<b>Abstract</b> see report		
<b>Subject Terms</b>		
<b>Report Classification</b> unclassified		<b>Classification of this page</b> unclassified
<b>Classification of Abstract</b> unclassified		<b>Limitation of Abstract</b> SAR
<b>Number of Pages</b> 46		



# CRITICAL INFRASTRUCTURE PROTECTION

## Significant Homeland Security Challenges Need to Be Addressed

Highlights of [GAO-02-918T](#), testimony before the Subcommittee on Oversight and Investigations, House Committee on Energy and Commerce.

### Why GAO Did This Study

Since the terrorist attacks of last September 11, the President and the Congress have taken important, aggressive action to protect the nation. Last month, the President proposed elevating homeland security to department status and, at the same time, merging into it several federal organizations. It would comprise four divisions (see graphic).

The six organizations to be moved into the new department's Information Analysis and Infrastructure Protection division (and their current parent organizations) are the National Infrastructure Protection Center (FBI), National Communications System (Defense), Critical Infrastructure Assurance Office (Commerce), Computer Security Division (National Institute of Standards and Technology), National Infrastructure Simulation and Analysis Center (Defense, Energy), and the Federal Computer Incident Response Center (General Services Administration).

At the Subcommittee's request, GAO discussed the functions to be transferred to this new division, along with the potential benefits to be achieved, and the challenges that it will likely face.

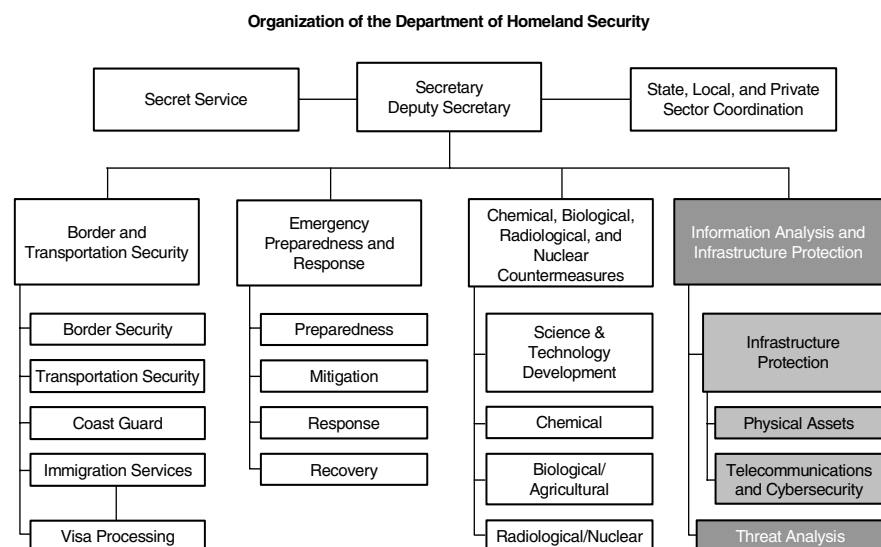
### What GAO Found

As proposed, the functions of the Information Analysis and Infrastructure Protection division would include receiving and analyzing law enforcement and intelligence information, assessing cyber and physical vulnerabilities of critical infrastructures, and taking measures to protect them.

The consolidation of these six organizations into a single division, if properly implemented, could result in combining similar functions, thereby avoiding duplication and possibly creating more robust capabilities. For example, analysis and warning of cyber incidents is currently performed by both the National Infrastructure Protection Center and the Federal Computer Incident Response Center.

However, prior GAO work has identified and made recommendations concerning several critical infrastructure protection challenges that need to be addressed, which would face the new department. Specifically, they are:

- *Developing a national critical infrastructure protection strategy.*
- *Improving analytical and warning capabilities.*
- *Improving information sharing.*
- *Addressing pervasive weaknesses in federal information security.*



---

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the proposed reorganization of government agencies and the reorientation of their missions to improve our nation's ability to better protect our homeland. This historical transition is clearly one of the most important issues of our time and is already being compared to other large-scale government reorganizations, including the creation of the Department of Defense, the Central Intelligence Agency, and the National Security Council as part of the National Security Act of 1947.

In the months since the events of September 11, the President and the Congress have responded with important and aggressive actions to protect the nation—creating the Office of Homeland Security and the Critical Infrastructure Protection Board, passing new laws such as the USA Patriot Act and an emergency supplemental spending bill, establishing a new agency to improve transportation security, and working in collaboration with federal, state, and local governments and private sector entities to prevent future terrorist acts. More recently, the Congress and the President have sought to remedy long-standing issues and concerns in the government's homeland security functions by proposing greater consolidation and coordination of various agencies and activities. Recent proposals include restructuring the Federal Bureau of Investigation (FBI) and splitting the enforcement and service sections of the Immigration and Naturalization Service (INS). Additionally, Senator Joseph I. Lieberman and Representative William M. “Mac” Thornberry have authored legislation designed to consolidate many homeland security functions.

On June 18, the President transmitted draft legislation to the Congress for the creation of a new Department of Homeland Security whose mission would be preventing terrorist attacks within the United States, reducing America's vulnerability to terrorism, and minimizing the damage and recovering from attacks that do occur. The Comptroller General recently testified on issues that Congress should review in its deliberations on creating the new cabinet department.<sup>1</sup> Specifically, the Comptroller General discussed (1) the need for reorganization and the principles and criteria to help evaluate what agencies and missions should be included or

---

<sup>1</sup>U.S. General Accounting Office, *Homeland Security: Proposal for Cabinet Agency Has Merit, But Implementation Will be Pivotal to Success*; [GAO-02-886T](#) (Washington, D.C.: June 25, 2002).

---

excluded from the new department, and (2) issues related to transition, cost, and implementation challenges.

The new cabinet department would incorporate several federal organizations, including the U.S. Secret Service and the U.S. Coast Guard, and would be organized into four divisions: (1) Information Analysis and Infrastructure Protection; (2) Chemical, Biological, Radiological and Nuclear Countermeasures; (3) Border and Transportation Security; and (4) Emergency Preparedness and Response. In particular, the Information Analysis and Infrastructure Protection division will perform one of the department's most critical missions: analyzing information and intelligence to better foresee terrorist threats to the United States.

Today, as requested, I will discuss the specific functions that would be performed by the department's Information Analysis and Infrastructure Protection division and the organizations that would be transferred to this division. I will also discuss the potential benefits and challenges for this division and, as indicated by our past reports on critical infrastructure protection (CIP) and federal information security, other major challenges that the new department would face. CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are essential to national security, national economic security, and/or national public health and safety.

In preparing this testimony, we relied on prior GAO reports and testimonies on critical infrastructure protection, information security, and national preparedness, among others. We reviewed and analyzed the President's proposal to establish the Department of Homeland Security and the draft legislation. We also met with officials at the Department of Commerce's Critical Infrastructure Assurance Office and the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center to follow up on prior recommendations and to discuss their proposed move to the new department. Our work was performed in accordance with generally accepted government auditing standards.

---

## Results in Brief

As proposed, functions of the Homeland Security Department's Information Analysis and Infrastructure Protection Division would include (1) receiving and analyzing law enforcement information, intelligence, and other information to detect and identify potential threats of terrorism within the United States; (2) assessing the vulnerabilities of the key resources and critical infrastructures in the United States; (3) developing a comprehensive national plan for securing these resources and

infrastructures; and (4) taking necessary measures to protect these resources and infrastructures, in coordination with other executive agencies and in cooperation with state and local government personnel, agencies, and authorities, the private sector, and other entities. To create this division, six federal organizations that currently play a pivotal role in the protection of our national critical infrastructures would be transferred to this division in the new department. These organizations and their current parent organizations are shown in table 1.

**Table 1: Organizations to Be Moved to Information Analysis and Infrastructure Protection Division**

Organization to be moved	Current parent organization
National Infrastructure Protection Center (NIPC) <sup>a</sup>	FBI
National Communications System (NCS)	Department of Defense (DOD) <sup>b</sup>
Critical Infrastructure Assurance Office (CIAO)	Department of Commerce
Computer Security Division	National Institute of Standards and Technology (NIST)
National Infrastructure Simulation and Analysis Center	DOD/Department of Energy (DOE)
Federal Computer Incident Response Center (FedCIRC)	General Services Administration (GSA)

<sup>a</sup>The Computer Investigations and Operations Section currently within NIPC would remain at the FBI.

<sup>b</sup>DOD is the executive agent for the NCS, which reports to multiple Executive Office of the President organizations.

The consolidation of essential CIP functions and organizations may, if properly organized and implemented, lead over time to more efficient, effective, and coordinated programs. For example, two of the organizations proposed for consolidation—the GSA’s FedCIRC and the FBI’s NIPC—conduct incident reporting, analysis, and warning functions. Combining such efforts could not only eliminate possible duplicative efforts, but might also result in stronger and more coordinated capabilities. Other potential benefits include better control of funding through a single appropriation process for the new department and through establishing budget priorities for transferred functions based on their homeland security mission, and the consolidation of points of contact for federal agencies, state and local governments, and the private sector in coordinating activities to protect our homeland.

The Information Analysis and Infrastructure Protection Division will also face implementation challenges. For example, the new department will

---

face tremendous information management and technology challenges, not the least of which will be integrating the diverse communications and information systems of the programs and agencies being brought together and securing the sensitive information these networks and systems process.

Further, through our past work, we have identified other significant challenges for many aspects of the functions to be transferred to the Information Analysis and Infrastructure Protection Division, and have recommended numerous changes to improve information analysis and protect our critical infrastructures. These challenges, which would face the new department, include the following:

- *Developing a national CIP strategy.* Although steps have been taken in this direction, a more complete strategy is needed that will address specific CIP roles and responsibilities for entities both within and outside of the new department, clearly define interim objectives and milestones, set time frames for achieving objectives, establish performance measures, and clarify how CIP entities will coordinate their activities.
- *Improving analytical and warning capabilities.* Although improvement efforts have been initiated, more robust analysis and warning capabilities, including a methodology for strategic analysis and a framework for collecting needed threat and vulnerability information, are still needed to identify threats and provide timely warnings. Such capabilities need to include both cyber and physical threats.
- *Improving information sharing on threats and vulnerabilities.* Information sharing needs to be improved both within the government and between the federal government and the private sector and state and local governments.
- *Addressing pervasive weaknesses in federal information security.* A comprehensive strategy for improving federal information security is needed, in which roles and responsibilities are clearly delineated, appropriate guidance is given, regular monitoring is undertaken, and security information and expertise are shared to maximize their value.

---

## Critical Infrastructure Protection Policy Has Been Evolving Since the Mid-1990's

Federal awareness of the importance of securing our nation's critical infrastructures, which underpin our society, economy, and national security, has been evolving since the mid-1990's. Over the years, a variety of working groups have been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. In October 1997, the President's Commission on Critical Infrastructure Protection issued its report,<sup>2</sup> which described the potentially devastating implications of poor information security from a national perspective. The report recommended several measures to achieve a higher level of critical infrastructure protection, including infrastructure protection through industry cooperation and information sharing, a national organization structure, a revised program of research and development, a broad program of awareness and education, and reconsideration of laws related to infrastructure protection. The report stated that a comprehensive effort would need to "include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyberthreats." It said that the FBI had already begun to develop warning and threat analysis capabilities and urged it to continue in these efforts. In addition, the report noted that the FBI could serve as the preliminary national warning center for infrastructure attacks and provide law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

In 1998, the President issued Presidential Decision Directive (PDD) 63, which describes a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. PDD 63 called for a range of actions intended to improve federal agency security programs, improve the nation's ability to detect and respond to serious computer-based and physical attacks, and establish a partnership between the government and the private sector. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved and designated lead agencies to work with private-sector and government organizations. Further, it established critical infrastructure protection as a national goal, and stated that, by the close of 2000, the United States was to have achieved an initial operating capability to protect the nation's critical infrastructures from intentional destructive acts and, no later than 2003, an enhanced capability.

---

<sup>2</sup>*Critical Foundations: Protecting America's Infrastructures*, Report of the President's Commission on Critical Infrastructure Protection (October 1997).

---

To accomplish its goals, PDD 63 designated and established organizations to provide central coordination and support, including

- the Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies;
- the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response; and
- the National Infrastructure Assurance Council, which was established to enhance the partnership of the public and private sectors in protecting our critical infrastructures.<sup>3</sup>

To ensure coverage of critical sectors, PDD 63 also identified eight private-sector infrastructures and five special functions. The infrastructures are (1) information and communications; (2) banking and finance; (3) water supply; (4) aviation, highway, mass transit, pipelines, rail, and waterborne commerce; (5) emergency law enforcement; (6) emergency fire services and continuity of government; (7) electric power and oil and gas production and storage; and (8) public health services. The special functions are (1) law enforcement and internal security, (2) intelligence, (3) foreign affairs, (4) national defense, and (5) research and development. For each of the infrastructures and functions, the directive designated lead federal agencies to work with their counterparts in the private-sector. For example, the Department of the Treasury is responsible for working with the banking and finance sector, and the Department of Energy is responsible for working with the electrical power industry. Similarly, regarding special function areas, DOD is responsible for national defense, and the Department of State is responsible for foreign affairs.

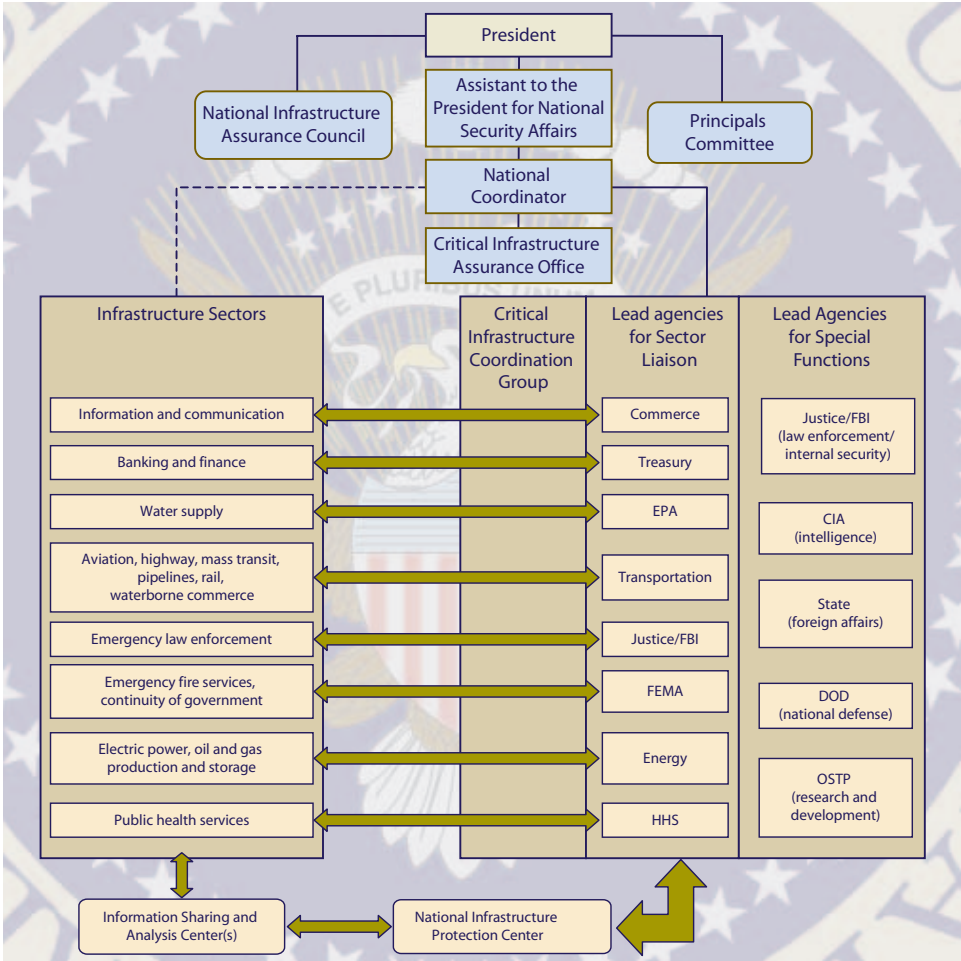
To facilitate private-sector participation, PDD 63 also encouraged the creation of information sharing and analysis centers (ISACs) that could serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through the NIPC. Figure 1 displays a high-level

---

<sup>3</sup>Executive Order 13231 replaces this council with the National Infrastructure Advisory Council.

overview of the organizations with CIP responsibilities as outlined by PDD 63.

Figure 1: Organizations with CIP Responsibilities as Outlined by PDD 63



Note: In February 2001, the Critical Infrastructure Coordination Group was replaced by the Information Infrastructure Protection and Assurance Group under the Policy Coordinating Committee on Counter-terrorism and National Preparedness. In October 2001, the National Infrastructure Assurance Council was replaced by the National Infrastructure Advisory Council, and cyber CIP functions performed by the national coordinator were assigned to the chair of the President's Critical Infrastructure Protection Board.

Source: CIAO.

---

In response to PDD 63, in January 2000 the White House issued its “National Plan for Information Systems Protection.”<sup>4</sup> The national plan provided a vision and framework for the federal government to prevent, detect, respond to, and protect the nation’s critical cyber-based infrastructure from attack and reduce existing vulnerabilities by complementing and focusing existing federal computer security and information technology requirements. Subsequent versions of the plan were expected to (1) define the roles of industry and state and local governments working in partnership with the federal government to protect physical and cyber-based infrastructures from deliberate attack and (2) examine the international aspects of CIP.

The most recent federal CIP guidance was issued in October 2001, when President Bush signed Executive Order 13231, establishing the President’s Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation’s critical infrastructures. The Special Advisor to the President for Cyberspace Security chairs the board. Executive Order 13231 tasks the board with recommending policies and coordinating programs for protecting CIP-related information systems. The executive order also established 10 standing committees to support the board’s work on a wide range of critical information infrastructure efforts. The board is intended to coordinate with the Office of Homeland Security in activities relating to the protection of and recovery from attacks against information systems for critical infrastructure, including emergency preparedness communications that were assigned to the Office of Homeland Security by Executive Order 13228, dated October 8, 2001. The board recommends policies and coordinates programs for protecting information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. In addition, the chair coordinates with the Assistant to the President for Economic Policy on issues relating to private-sector systems and economic effects and with the Director of OMB on issues relating to budgets and the security of federal computer systems. Further, the Special Advisor reports to the Assistant to the President for National Security Affairs and to the Assistant to the President for Homeland Security.

---

<sup>4</sup>The White House, *Defending America’s Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* (Washington, D.C.: 2000).

---

## Implementing PDD 63 Has Not Been Completely Successful

Both GAO and the inspectors general have issued reports highlighting concerns about PDD 63 implementation. As we reported in September 2001, efforts to perform substantive, comprehensive analyses of infrastructure sector vulnerabilities and development of related remedial plans had been limited. Further, a March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in federal agencies' implementation of PDD 63 requirements to (1) establish plans for protecting their own critical infrastructure that were to be implemented within 2 years, or by May 2000, and (2) develop procedures and conduct vulnerability assessments.<sup>5</sup>

Specifically,

- many agency critical infrastructure protection plans were incomplete and some agencies had not developed such plans,
- most agencies had not completely identified their mission-essential infrastructure assets, and
- few agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

Our subsequent review of PDD 63-related activities at eight lead agencies found similar problems, although some agencies had made progress since their respective inspectors general reviews.<sup>6</sup> Further, OMB reported in February 2002 that it planned to direct all large agencies to undertake a Project Matrix review to identify critical infrastructure assets and their interdependencies with other agencies and the private sector.<sup>7</sup>

We identified several other factors that had impeded federal agency efforts to comply with PDD 63. First, no clear definitions had been developed to guide development and implementation of agency plans and measure performance. For example, PDD 63 established December 2000 as the

---

<sup>5</sup>The PCIE primarily is comprised of the presidentially appointed inspectors general and the ECIE is primarily comprised of the agency head-appointed inspectors general. In November 1999, PCIE and ECIE formed a working group to review the adequacy of federal agencies' implementation of PDD 63. The March 2001 report is based on reviews by 21 inspectors general of their respective agencies' PDD 63 planning and assessment activities.

<sup>6</sup>GAO-01-822, September 20, 2001.

<sup>7</sup>Project Matrix is a CIAO methodology that identifies all critical assets, nodes, networks, and associated infrastructure dependencies and interdependencies.

---

deadline for achieving an initial operating capability and May 2003 for achieving full operational capability of key functions. However, the specific capabilities to be achieved at each milestone had not been defined. The PCIE/ECIE report noted that agencies had used various interpretations of initial operating capability and stated that, without a definition, there is no consistent measure of progress toward achieving full security preparedness. In addition, several agency officials said that funding and staffing constraints contributed to their delays in implementing PDD 63 requirements. Further, the availability of adequate technical expertise to provide information security has been a continuing concern to agencies.

---

## Cyber Threats Are Increasing

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often on a 24-hour-a-day basis; and electronic mail, Internet web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, and national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. The speed and accessibility that create the enormous benefits of the computer age likewise, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping

---

sniffers that can destroy, intercept, degrade the integrity of, or deny access to data. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests. In addition, the disgruntled organization insider is a significant threat, since such individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions.

Reports of attacks and disruptions abound. The 2002 report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad, showed that 90 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months. In addition, the number of computer security incidents reported to the CERT® Coordination Center rose from 9,859 in 1999 to 52,658 in 2001 and 26,829 for just the first quarter of 2002. And these are only the reported attacks.<sup>8</sup> The CERT® Coordination Center estimates that as much as 80 percent of actual security incidents go unreported, in most cases because the organization was unable to recognize that its systems had been penetrated or because there were no indications of penetration or attack.

Since the September 11 attacks, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, earlier this year, the Special Advisor to the President for Cyberspace Security stated in a Senate briefing that although to date none of the traditional terrorist groups such as al Qaeda have used the Internet to launch a known attack on the United States infrastructure, information on computerized water systems was recently discovered on computers found in al Qaeda camps in Afghanistan. Further, in his October congressional testimony, Governor James Gilmore, Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (commonly known as the "Gilmore Commission"), warned

---

<sup>8</sup>CERT® Coordination Center (CERT-CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

---

that systems and services critical to the American economy and the health of our citizens—such as banking and finance, “just-in-time” delivery systems for goods, hospitals, and state and local emergency services—could all be shut down or severely handicapped by a cyber attack or a physical attack against computer hardware.<sup>9</sup>

---

## Information Analysis and Infrastructure Protection Division Consolidates Several CIP Functions

On June 6, President Bush announced a new proposal to create a Department of Homeland Security and submitted draft legislation to Congress on June 18. Like the congressional approaches to create a new department, the President’s plan also reflected many of the recent commissions’ suggestions and our recommendations for improved coordination and consolidation of homeland security functions. As indicated by Governor Ridge is his recent testimony before Congress, the creation of this department would empower a single cabinet official whose primary mission is to protect the American homeland from terrorism, including: (1) preventing terrorist attacks within the United States; (2) reducing America’s vulnerability to terrorism; and (3) minimizing the damage and recovering from attacks that do occur.<sup>10</sup>

In our initial review of the proposed department, we have used the President’s draft bill of June 18 as the basis of our comments. Nevertheless, we recognize that the proposal has already—and will continue—to evolve in the coming days and weeks ahead. The President’s proposal creates a cabinet department with four divisions, including:

- Information Analysis and Infrastructure Protection;
- Chemical, Biological, Radiological and Nuclear Countermeasures;
- Border and Transportation Security; and
- Emergency Preparedness and Response.

One of the most critical functions that the new department will have is the analysis of information and intelligence to better foresee terrorist threats to the United States—a function that would be performed by the

---

<sup>9</sup>Testimony of Governor James S. Gilmore III, Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction before the House Science Committee, October 17, 2001.

<sup>10</sup>*The Department of Homeland Security: Making Americans Safer*, Written Statement of Governor Tom Ridge before the Committee on Governmental Affairs, U.S. Senate, June 20, 2002.

---

Information Analysis and Infrastructure Protection Division. The primary responsibilities of this division would be

- receiving and analyzing law enforcement information, intelligence, and other information in order to understand the nature and scope of the terrorist threat to the American homeland and to detect and identify potential threats of terrorism within the U.S;
- assessing the vulnerabilities of the key resources and critical infrastructures in the United States including food and water systems, agriculture, health systems, emergency services, banking and finance, communications and information systems, energy (including electric, nuclear, gas and oil and hydropower), transportation systems, and national monuments;
- integrating relevant information, intelligence analyses, and vulnerability assessments to identify protective priorities and support protective measures by the Department, by other executive agencies, by state and local government personnel, agencies, and authorities, by the private sector, and by other entities;
- developing a comprehensive national plan for securing the key resources and critical infrastructures in the United States;
- taking or seeking to effect necessary measures to protect the key resources and critical infrastructures in the United States, in coordination with other executive agencies and in cooperation with state and local government personnel, agencies, and authorities, the private sector, and other entities;
- administering the Homeland Security Advisory System, exercising primary responsibility for public threat advisories, and (in coordination with other executive agencies) providing specific warning information to state and local government personnel, agencies, and authorities, the private sector, other entities, and the public, as well as advice about appropriate protective actions and countermeasures; and
- reviewing, analyzing, and making recommendations for improvements in the policies and procedures governing the sharing of law enforcement, intelligence, and other information relating to homeland security within the federal government and between such government and state and local government personnel, agencies, and authorities.

To create this division, the proposed reorganization would transfer six federal organizations that currently play a pivotal role in the protection of our national critical infrastructures—the FBI’s National Infrastructure Protection Center (other than the computer investigations and operations center), DOD’s National Communications System, the Commerce Department’s Critical Infrastructure Assurance Office, the Computer

---

Security Division of Commerce's NIST, the National Infrastructure Simulation and Analysis Center of DOD/DOE, and GSA's FedCIRC. (See the appendix for a description of the principal activities of these six organizations.)

---

## Potential Benefits Could Be Achieved By Consolidating Similar Activities

The administration has indicated that this new division would for the first time merge under one roof the capability to identify and assess threats to the homeland, map those threats against our vulnerabilities, issue timely warnings, and organize preventive or protective action to secure the homeland. The agencies and programs included in the Administration's proposal to consolidate information analysis functions are clear contributors to the homeland security mission and, if well coordinated or consolidated, could provide greater benefits by avoiding duplication and more closely coordinating activities.

Three areas are clearly opportunities for synergy: outreach and education; the identification of critical assets; and incident reporting, analysis, and warning. Currently the NIPC and CIAO both provide outreach to educate groups regarding the importance of protecting our critical infrastructures. These two organizations are also involved in the identification of critical assets. For instance, the NIPC is responsible for the Key Asset Initiative—a database of the most important components of the nation's critical infrastructures—while the CIAO is responsible for Project Matrix—a methodology that identifies all critical assets, nodes, networks, and associated infrastructure dependencies and interdependencies. Further, both the NIPC and FedCIRC have threat identification, incident reporting, analysis, and warning responsibilities. The CIAO Director recently testified that the new division will combine functions that are currently fragmented and inefficient, minimize duplication or redundancy of efforts, and ensure that critical infrastructure and cyber security activities can be more closely coordinated.

Several other potential benefits could be realized with the consolidation of related organizations and responsibilities within a single department. First, funding for critical infrastructure protection activities of the transferred organizations such as the NIPC and the CIAO could be better controlled through a single appropriation process rather than through separate processes for different departments. For example, as we reported in April 2001, NIPC's budget requests—including staffing and other financial resources—are controlled by the FBI and the Department of Justice, raising concern at that time among NIPC officials that its priorities, which are intended to reflect the interests of national critical infrastructure

---

protection, may be subordinated to the FBI's law enforcement priorities. NIPC officials told us that the FBI had not approved their repeated requests for additional resources as part of the budget process. Another potential benefit is the consolidation of points of contact for use by other federal agencies, state and local governments, the private sector, and other entities so that those within and external to the federal government have a clear understanding of whom to coordinate with on homeland security issues.

---

## New Department Needs to Focus on Critical Success Factors

In his June 2002 testimony, the Comptroller General noted key factors that should be considered for successfully implementing the new department.<sup>11</sup> These key factors include strategic planning, organizational alignment, communication and building partnerships, performance management, human capital strategy, information management and technology, knowledge management, financial management, acquisition management, and risk management. Given the transfer of organizations and responsibilities, the analysis and assessment functions to be performed, and the sensitivity of information to be collected, several of these factors will also be particularly important for the proposed Information Analysis and Infrastructure Protection Division. Specifically:

**Human capital strategy.** An organization's people are its most important asset. People define an organization, affect its capacity to perform, and represent the knowledge base of the organization. In an effort to help agency leaders integrate human capital considerations into daily decision-making and in the program results they seek to achieve, we have recently released an exposure draft of a model of strategic human capital management that highlights the kinds of thinking that agencies should apply and steps they can take to manage their human capital more strategically.<sup>12</sup> The model focuses on four cornerstones for effective human capital management—leadership; strategic human capital planning; acquiring, developing, and retaining talent; and results-oriented organization culture—and both the new department and the new division may find this model useful in helping guide its efforts. Hiring and retaining personnel with appropriate technology and analytical skills will also be critical to the new division.

---

<sup>11</sup>GAO-02-886T, June 25, 2002.

<sup>12</sup>U.S. General Accounting Office, *A Model of Strategic Human Capital Management*, GAO-02-373SP (Washington, D.C.: Mar. 15, 2002).

---

**Information management and technology.** The new department will face significant information management and technology challenges. Programs and agencies will be brought together in the new department from throughout the government, and each will bring their own communications and information systems. It will be a tremendous undertaking to integrate these diverse systems and enable effective communication and share information among themselves, as well as those outside the department.

To address the challenge, it will be critical that an enterprise architecture be developed to guide the integration and modernization of information systems. Such architecture, required by the Clinger-Cohen Act, consist of models that describe how the enterprise operates now and how it needs to operate in the future. Without an enterprise architecture to guide and constrain information technology investments, stovepipe operations and systems can emerge, which in turn lead to needless duplication, incompatibilities, and additional costs. This will be quite a challenge given that, as we reported earlier this year, few federal departments and agencies have the management practices necessary to develop and leverage enterprise architectures.<sup>13</sup> It will be particularly important for the new division to leverage technology to enhance its ability to transform capabilities and capacities to share and act upon timely, quality information about terrorist threats.

Further, as discussed later, since 1996, we have reported that poor information security is a widespread federal government problem with potentially devastating consequences. Considering the sensitivity of the data at the proposed department, securing its information systems and networks will be of utmost importance.

---

## Proposed Homeland Security Department Faces Ongoing Challenges

We have reported for years on many aspects of the functions that are to be transferred to the Information Analysis and Infrastructure Protection division and have made numerous recommendations to improve information analysis and to protect our critical infrastructures. Specific challenges, which would face the new department, include developing a national CIP strategy, improving analytical and warning capabilities,

---

<sup>13</sup>U.S. General Accounting Office, *Information Technology: Enterprise Architecture Use Across the Federal Government Can Be Improved*, [GAO-02-6](#) (Washington, D.C.: Feb. 19, 2002).

---

improving information sharing, and addressing pervasive weaknesses in federal information security.

---

## National CIP Strategy Needs to Be Developed

A clearly defined strategy is essential for defining the relationships among all CIP organizations, both internal as well as external to the proposed Department of Homeland Security, to ensure that the approach is comprehensive and well coordinated. The President's proposal states that one of the primary responsibilities of the new Information Analysis and Infrastructure Protection division is to develop such a strategy.

An underlying issue in the implementation of PDD 63, and a major challenge for the new department, is that no national strategy yet exists that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities and defines interim objectives.<sup>14</sup> We first identified the need for a detailed plan in September 1998, when we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of new and existing federal entities was important to ensure governmentwide cooperation and support for PDD 63.<sup>15</sup> At that time, we recommended that OMB and the Assistant to the President for National Security Affairs ensure such coordination.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public/private partnership to defend our national infrastructures by achieving three crosscutting infrastructure protection objectives:

- minimize the possibility of significant and successful attacks;
- identify, assess, contain, and quickly recover from an attack; and
- create and build strong foundations, including people, organizations, and laws, for preparing, preventing, detecting and responding to attacks.

---

<sup>14</sup>GAO-01-822, September 20, 2001.

<sup>15</sup>U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*; GAO/AIMD-98-92 (Washington, D.C.: Sep. 23, 1998).

---

However, this plan focused largely on federal cyber CIP efforts, saying little about the private-sector role. Subsequently, in July 2000, we reiterated the importance of defining and clarifying organizational roles and responsibilities, noting that numerous federal entities were collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents and that clarification would help ensure a common understanding of (1) how the activities of these many organizations interrelate, (2) who should be held accountable for their success or failure, and (3) whether such activities will effectively and efficiently support national goals.<sup>16</sup>

A May 2001 White House press statement announced that the administration was reviewing how it was organized to deal with information security issues and that recommendations would be made on how to structure an integrated approach to cyber security and critical infrastructure protection. Specifically, the announcement stated that the White House, federal agencies, and private industry had begun to collaboratively prepare a new version of a “national plan for cyberspace security and critical infrastructure protection” and reviewing how the government is organized to deal with information security issues.

In September 2001, we reported that agency questions had surfaced regarding specific roles and responsibilities of entities involved in cyber CIP and the timeframes within which CIP objectives are to be met, as well as guidelines for measuring progress.<sup>17</sup> Accordingly, we made several recommendations to supplement those we had made in the past, including those regarding the NIPC. Specifically, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government’s strategy to address computer-based threats define

- specific roles and responsibilities of organizations involved in critical infrastructure protection and related information security activities;
- interim objectives and milestones for achieving critical infrastructure protection goals and a specific action plan for achieving these objectives, including implementation of vulnerability assessments and related remedial plans; and

---

<sup>16</sup>U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination*; [GAO/T-AIMD-00-268](#) (Washington, D.C.: July 26, 2000).

<sup>17</sup>[GAO-01-822](#), September 20, 2001.

- 
- performance measures for which entities can be held accountable. The national strategy for cyber CIP is still being developed and is now planned to be issued in September 2002.

Further, an important aspect of this strategy will be the inclusion of all CIP-related federal activities. For example, it should include additional sectors not included in PDD 63. This was acknowledged by the chair of the President's Critical Infrastructure Protection Board recently, when he told a Senate subcommittee that the critical infrastructure sectors were being reviewed after the September 11 attacks and the subsequent anthrax attacks on the U.S. Capitol. In addition, the proposal to create a Department of Homeland Security refers to the need to consider additional sectors. According to the proposal, "the Department would be responsible for comprehensively evaluating the vulnerabilities of America's critical infrastructure, including food and water systems, agriculture, health systems and emergency services, information and telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons." It is also important that any CIP-related efforts or proposals outside the current scope of PDD 63 be coordinated with other CIP efforts. For example, we understand that EPA is considering a proposal that would require the 15,000 industrial facilities using hazardous chemicals to submit detailed vulnerability assessments.

A clearly defined strategy is also essential for clarifying how CIP entities will coordinate their activities with each other, both those that are to be included in the proposed department and those external to it. For example, Information Analysis and Infrastructure Protection division's responsibilities include receiving and analyzing law enforcement information, intelligence, and other information. Similar functions are also performed by the recently created Transportation Security Agency, which the bill transfers to another division of the new department. Coordinating these similar activities within the new department will be critical to avoiding unnecessarily duplicative efforts and ensuring the effective flow of appropriate law enforcement, intelligence, and other information to the entities that need it. In addition, the numerous federal CIP organizations that will remain in place, such as the President's Critical Infrastructure Protection Board, NIPC's Computer Investigations and Operations Section that is to remain with the FBI, and the Joint Task Force for Computer Network Operations within the Department of Defense will need to be closely coordinated with the other CIP players. Coordination will be especially critical between the department and the other federal entities

---

that are to provide it with intelligence and other threat information, such as the FBI and the CIA.

A national strategy that covers both cyber and physical CIP could greatly facilitate such organizational coordination and the success of the new department. CIAO officials told us that separate cyber and physical strategies are now planned to be issued. Without a comprehensive and coordinated strategy that identifies roles and responsibilities for all CIP efforts, our nation risks not having a consistent and appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructure.

---

## Analytical and Warning Capabilities Need to Be Improved

Another key challenge for the new department is to develop the analysis and warning capabilities called for in the President's proposal. NIPC was established in PDD 63 as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. Specifically, the directive assigned the NIPC the responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to computer-based incidents; providing law enforcement investigation and response, monitoring reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing. This responsibility requires obtaining and analyzing intelligence, law enforcement, and other information to identify patterns that may signal that an attack is underway or imminent. Similar activities are also called for in the President's proposal for the Information Analysis and Infrastructure Protection division.

In April 2001, we reported on NIPC's progress in developing national capabilities for analyzing threat and vulnerability data and issuing warnings, responding to attacks, among others.<sup>18</sup> Overall, we found that while progress in developing these capabilities was mixed, the NIPC had initiated a variety of critical infrastructure protection efforts that had laid a foundation for future governmentwide efforts. In addition, the NIPC had provided valuable support and coordination related to investigating and

---

<sup>18</sup>U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*; [GAO-01-323](#) (Washington, D.C.: Apr. 25, 2001).

---

otherwise responding to attacks on computers. However, at the close of our review, the analytical capabilities that PDD 63 asserted are needed to protect the nation's critical infrastructures had not yet been achieved, and the NIPC had developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

At the time of our review, the NIPC had issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. In addition, it had issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis.

We reported that the use of strategic analysis to determine the potential broader implications of individual incidents had been limited. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. Identifying such threats assists in proactively managing risk, including evaluating the risks associated with possible future incidents and effectively mitigating the impact of such incidents.

We reported last year that three factors hindered NIPC's ability to develop strategic analytical capabilities:

- First, there was no generally accepted methodology for analyzing strategic cyber-based threats. For example, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.
- Second, the NIPC had sustained prolonged leadership vacancies and did not have adequate staff expertise, in part because other federal agencies had not provided the originally anticipated number of detailees. For example, at the close of our review in February, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of NIPC's 3-year existence. In addition, the NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimate are needed to develop analytical capabilities.
- Third, the NIPC did not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight

---

industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work, only three industry assessments had been partially completed, and none had been provided to the NIPC.

To provide a warning capability, the NIPC established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. While some warnings were issued in time to avert damage, most of the warnings, especially those related to viruses, pertained to attacks underway. We reported that NIPC's ability to issue warnings promptly was impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks, (2) a shortage of skilled staff, (3) the need to ensure that the NIPC does not raise undue alarm for insignificant incidents, and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway.

Further, the relationships between the Center, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council were unclear regarding who had direct authority for setting NIPC priorities and procedures and providing NIPC oversight. In addition, NIPC's own plans for further developing its analytical and warning capabilities were fragmented and incomplete. As a result, no specific priorities, milestones, or program performance measures existed to guide NIPC's actions or provide a basis for evaluating its progress.

In our report, we recognized that the administration was reviewing the government's infrastructure protection strategy and recommended that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategically analyzing computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data;
- require development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources, and
- clearly define the role of the NIPC in relation to other government and private-sector entities.

---

In response to our report recommendations, the NIPC Director recently told us that NIPC had developed a plan with goals and objectives to improve their analytical and warning capabilities and that NIPC has made considerable progress in this area. For example, the Director told us that the analysis and warning section has created two additional teams to bolster its analytical capabilities—(1) the critical infrastructure assessment team to focus efforts on learning about particular infrastructures and coordinating with respective infrastructure efforts and (2) the collection operations intelligence liaison team to coordinate with various entities within the intelligence community. The Director added that NIPC (1) now holds a quarterly meeting with senior government leaders of entities that it regularly works with to better coordinate their analytical and warning capabilities, (2) has developed close working relationships with other CIP entities involved in analysis and warning activities, such as FedCirc, DOD's Joint Task Force for Computer Network Operations, the Carnegie Mellon's Computer Emergency Response Team (CERT) Coordination Center, and the intelligence and anti-virus communities, and (3) had developed and implemented procedures to more quickly share relevant CIP information, while separately continuing any related law enforcement investigation. The Director also stated that NIPC has received sustained leadership commitment from key entities, such as CIA and NSA, and that it continues to increase its staff primarily through reservists and contractors. The Director acknowledged that our recommendations are not fully implemented and that despite the accomplishments to date, much more work remains to create the robust analysis and warning capabilities needed to adequately address cyberthreats.

Another challenge confronting the analysis and warning capabilities of the new department is that the functions proposed to be transferred to the new department for Information Analysis and Infrastructure Protection have historically focused their attention and efforts on cyber threats. In April 2001, we reported that while PDD 63 covers both physical and computer-based threats, federal efforts to meet the directive's requirements have pertained primarily to computer-based threats, since this was an area that the leaders of the administration's critical infrastructure protection strategy viewed as needing attention. Not only is physical protection of our critical infrastructures important in and of itself, but a physical attack in conjunction with a cyber attack has recently been highlighted as a major concern. Also, exploiting cyber vulnerabilities can be used as a means to attack our nation's critical physical infrastructures. The Director told us that NIPC had begun to develop some capabilities for the identification of physical CIP threats. For example, NIPC has

---

developed thresholds with several ISACs for reporting physical incidents and has, since January 2002, issued several information bulletins concerning physical CIP threats. However, NIPC Director acknowledged that fully developing this capability will be a significant challenge. It is important that the national CIP strategy adequately addresses physical threats.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, is received from the intelligence and law enforcement communities. For example, considerable debate has ensued in recent weeks with respect to the quality and timeliness of intelligence data shared between and among relevant intelligence, law enforcement, and other agencies. The proposal would provide for the new department to receive all reports and analysis related to threats of terrorism and vulnerabilities to our infrastructure and, if the President directs, information in the “raw” state that has not been analyzed. Also, with the proposed separation of NIPC from the FBI’s law enforcement activities, including the Counterterrorism Division and NIPC field agents, it will be critical to establish mechanisms for continued communication to occur. Further, it will be important that the relationships between the law enforcement and intelligence communities and the new department are effective and that appropriate information is exchanged on a timely basis.

Further, according to the NIPC Director, a significant challenge in developing a robust analysis and warning function is the development of the technology and human capital capacities to collect and analyze substantial amounts of information. Similarly, the Director of the FBI recently testified that implementing a more proactive approach to preventing terrorist acts and denying terrorist groups the ability to operate and raise funds requires a centralized and robust analytical capacity that does not currently exist in the FBI’s Counterterrorism Division. He also stated that processing and exploiting information gathered domestically and abroad during the course of investigations requires an enhanced analytical and data mining capacity that is not presently available. Also, the NIPC Director stated that multi-agency staffing, similar to NIPC, is a critical success factor in establishing an effective analysis and warning function and that appropriate funding for such staff was important.

---

## Government Faces Information Sharing Challenges

Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber attacks, which could threaten the national welfare. Information on threats and incidents experienced by others can help identify trends, better understand the risks faced, and determine what preventive measures should be implemented. However, as we testified in July 2000,<sup>19</sup> establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult. Last October we reported on information sharing practices that could benefit critical infrastructure protection.<sup>20</sup> These practices include

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents,
- developing standards and agreements on how shared information will be used and protected,
- establishing effective and appropriately secure communications mechanisms, and
- taking steps to ensure that sensitive information is not inappropriately disseminated, which may require statutory changes.

In June of this year, we also reported on the information sharing barriers confronting homeland security, both within the federal government and with the private sector.<sup>21</sup>

A number of activities have been undertaken to build relationships between the federal government and the private sector, such as InfraGard, the Partnership for Critical Infrastructure Security, efforts by the CIAO, and efforts by lead agencies to establish information sharing and analysis centers (ISACs). For example, the InfraGard Program, which provides the FBI and the NIPC with a means of securely sharing information with individual companies, has expanded substantially. By early January 2001, 518 entities were InfraGard members—up from 277 members in October 2000. Members included representatives from private industry, other

---

<sup>19</sup>[GAO/T-AIMD-00-268](#), July 26, 2000.

<sup>20</sup>U.S. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*; [GAO-02-24](#) (Washington, D.C.: Oct. 15, 2001).

<sup>21</sup>U.S. General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing Into an Effective Homeland Security Strategy*, [GAO-02-811T](#) (Washington, D.C.: June 7, 2002).

---

government agencies, state and local law enforcement, and the academic community. Currently, NIPC reports over 5,000 InfraGard members. Although each of these efforts is commendable, more needs to be done.

PDD 63 encouraged the voluntary creation of ISACs that could serve as the mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information between the private sector and the federal government through NIPC. Such centers are critical since the private sector entities control over 80 percent of our nation's critical infrastructures. In September 2001, we reported that although outreach efforts had raised awareness and improved information sharing, substantive, comprehensive analysis of infrastructure sector interdependencies, vulnerabilities and related remedial plans had been limited.

In April 2001, we reported that NIPC had undertaken a range of initiatives to foster information sharing relationships with ISACs, as well as government and international entities. We recommended that NIPC formalize relationships with ISACs and develop a plan to foster a two-way exchange of information between them. In response to our recommendations, NIPC officials told us that a new ISAC development and support unit had been created, whose mission is to enhance private sector cooperation and trust, resulting in a two-way sharing of information. NIPC now reports that 11 ISACs have been established, including those for the chemical industry, surface transportation, electric power, telecommunications, information technology, financial services, water supply, oil and gas, emergency fire services, food, and emergency law enforcement. Officials informed us that the Center has signed information sharing agreements with most ISACs, including those representing telecommunications, information technology, air transportation, water supply, food, emergency fire services, banking and finance, and chemical sectors. NIPC officials added that these agreements contained industry specific cyber and physical incident reporting thresholds. Further, officials told us that it has developed a program with the electric power ISAC whereby members transmit incident reports directly to NIPC.

Our ongoing work for this Subcommittee on five of these ISACs has shown that while progress has been made, each sector does not have a fully established ISAC, those that do have varied participation, and the amount

---

of information being shared between the federal government and private sector organizations also varies.<sup>22</sup> In the Comptroller General's testimony several weeks ago, he stated that intelligence and information sharing challenges highlight the need for strong partnerships with those outside the federal government and that the new department will need to design and manage tools of public policy (e.g., grants to non-federal entities) to engage and work constructively with third parties.<sup>23</sup>

Some in the private sector have expressed concerns about voluntarily sharing information with the government. For example, concerns have been raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information be subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith. Many suggest that the government should model the Year 2000 Information and Readiness Disclosure Act, which provided limited exemptions and protections for the private sector in order to facilitate the sharing of information on Year 2000 readiness.

In addition, other actions have been taken by the Congress and the administration to strengthen information sharing. The USA Patriot Act, for example, enhances or promotes information sharing among federal agencies, and numerous terrorism task forces have been established to coordinate investigations and improve communications among federal and local law enforcement. There will be continuing debate as to whether adequate protection is being provided to the private sector as these entities are encouraged to disclose and exchange information on both physical and cyber security problems and solutions that are essential to protecting our nation's critical infrastructures.

Information sharing within the government also remains a challenge. In April of last year, we reported that the NIPC and other government entities had not developed fully productive information sharing and cooperative relationships. For example, federal agencies had not routinely reported incident information to the NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to

---

<sup>22</sup>The five ISACs are information technology, telecommunications, energy, electricity, and water.

<sup>23</sup>[GAO-02-866T](#), June 25, 2002.

---

report such information to the General Services Administration's Federal Computer Incident Response Center. Further, NIPC and Defense officials agreed that their information-sharing procedures needed improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts. According to the NIPC director, the relationship between the NIPC and other government entities has significantly improved since our review, and that the quarterly meetings with senior government leaders have been instrumental in improving information sharing. In addition, officials from the Federal Computer Incident Response Center and the U.S. Secret Service in testimony have discussed the collaborative and cooperative relationships that now exist between their agencies and the NIPC.

---

## Pervasive Federal Information Security Weaknesses Need to Be Addressed

At the federal level, cyber CIP activities are a component, perhaps the most critical, of a federal department or agency's overall information security program. Federal agencies have significant critical infrastructures that need effective information security to adequately protect them. However, since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.<sup>24</sup> Our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in both 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies and found that all 24 agencies had significant information security weaknesses.<sup>25</sup> As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.<sup>26</sup> More current analyses of

---

<sup>24</sup>U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*; [GAO/AIMD-96-110](#) (Washington, D.C.: Sep. 24, 1996).

<sup>25</sup>U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*; [GAO/AIMD-98-92](#) (Washington, D.C.: Sep. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*; [GAO/AIMD-00-295](#) (Washington, D.C.: Sep. 6, 2000).

<sup>26</sup>U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*; [GAO/HR-97-9](#) (Washington, D.C.: Feb. 1, 1997); *High-Risk Series: An Update*; [GAO/HR-99-1](#) (Washington, D.C.: Jan. 1999); *High-Risk Series: An Update*, [GAO-01-263](#) (Washington, D.C.: Jan. 2001).

---

audit results, as well as of the agencies' own reviews of their information security programs continue to show significant weaknesses that put critical federal operations and assets at risk.

## Weaknesses Remain Pervasive

Our November 2001 analyses of audit results for 24 of the largest federal agencies showed that weaknesses continued to be reported in each of the 24 agencies.<sup>27</sup> These analyses considered GAO and inspector general (IG) reports published from July 2000 through September 2001, which included the first annual independent IG evaluations of agencies' information security programs required by government information security reform legislation (commonly referred to as "GISRA").<sup>28</sup>

Our analyses showed that the weaknesses reported for the 24 agencies covered all six major areas of general controls, that is, the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant

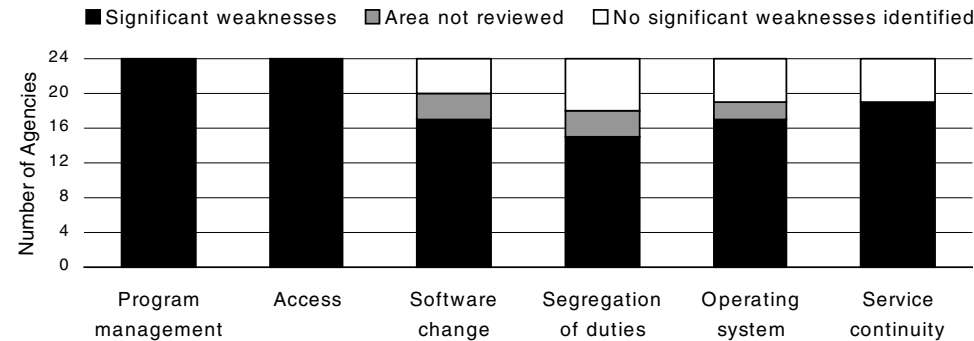
---

<sup>27</sup>U.S. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, [GAO-02-231T](#) (Washington, D.C.: Nov. 9, 2001).

<sup>28</sup>Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L. 106-398, October 30, 2000. Congress enacted "GISRA" to supplement information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and is consistent with existing information security guidance issued by OMB and the National Institute of Standards and Technology, as well as audit and best practice guidance issued by GAO. Most importantly, however, GISRA consolidates these separate requirements and guidance into an overall framework for managing information security and establishes new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight. Effective November 29, 2000, GISRA is in effect for 2 years after this date.

disruptions. Figure 2 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

**Figure 2: Information Security Weaknesses at 24 Major Agencies**



Source: Audit reports issued July 2000 through September 2001.

As in 2000, our current analysis shows that weaknesses were most often identified for security program management and access controls. For security program management, we found weaknesses for all 24 agencies in 2001 as compared to 21 of the 24 agencies (88 percent) in 2000. Security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls, covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively. For access controls, we also found weaknesses for all 24 agencies in 2001—the same condition we found in 2000. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today’s increasingly interconnected computing environment, poor access controls can expose an agency’s information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise. In 2001, we also found that 19 of the 24 agencies (79 percent) had weaknesses in service continuity controls (compared to 20 agencies or 83 percent in 2000). These controls are particularly important because they ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. If service continuity controls are inadequate, an agency can lose the capability to process, retrieve, and

---

protect electronically maintained information, which can significantly affect an agency's ability to accomplish its mission.

Our current analyses of information security at federal agencies also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. These increases in reported weaknesses do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 2 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily nonfinancial, such as the Departments of Defense and Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of individual systems supporting nonfinancial operations. In response to congressional interest, beginning in fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations—a trend we expect to continue. Audit coverage for nonfinancial systems is also likely to increase as agencies review and evaluate their information security programs as required by GISRA.

#### Weaknesses Pose Substantial Risks for Federal Operations, Assets, and Confidentiality

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high.

The weaknesses identified place a broad array of federal operations and assets at risk. For example,

- 
- resources, such as federal payments and collections, could be lost or stolen;
  - computer resources could be used for unauthorized purposes or to launch attacks on others;
  - sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime;
  - critical operations, such as those supporting national defense and emergency services, could be disrupted;
  - data could be modified or destroyed for purposes of fraud or disruption; and
  - agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Examples from recent audit reports issued in 2001 illustrate the serious weaknesses found in the agencies that continue to place critical federal operations and assets at risk:

- In August, we reported that significant and pervasive weaknesses placed Commerce's systems at risk. Many of these systems are considered critical to national security, national economic security, and public health and safety. Nevertheless, we demonstrated that individuals, both within and outside of Commerce, could gain unauthorized access to Commerce systems and thereby read, copy, modify, and delete sensitive economic, financial, personnel, and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department.<sup>29</sup> Commerce's IG has also reported significant computer security weaknesses in several of the department's bureaus and, in February 2001, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements.<sup>30</sup>
- In July, we reported serious weaknesses in systems maintained by the Department of Interior's National Business Center, a facility processing more than \$12 billion annually in payments that place sensitive financial

---

<sup>29</sup>U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*; [GAO-01-751](#) (Washington, D.C.: Aug. 13, 2001).

<sup>30</sup>Department of Commerce's Fiscal Year 2000 Consolidated Financial Statements, Inspector General Audit Report No. FSD-12849-1-0001.

---

and personnel information at risk of unauthorized disclosure, critical operations at risk of disruption, and assets at risk of loss. While Interior has made progress in correcting previously identified weaknesses, the newly identified weaknesses impeded the center's ability to (1) prevent and detect unauthorized changes, (2) control electronic access to sensitive information, and (3) restrict physical access to sensitive computing areas.<sup>31</sup>

- In March, we reported that although DOD's Departmentwide Information Assurance Program made progress, it had not yet met its goals of integrating information assurance with mission-readiness criteria, enhancing information assurance capabilities and awareness of department personnel, improving monitoring and management of information assurance operations, and establishing a security management infrastructure. As a result, DOD was unable to accurately determine the status of information security across the department, the progress of its improvement efforts, or the effectiveness of its information security initiatives.<sup>32</sup>
- In February, the Department of Health and Human Services' IG again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.<sup>33</sup> Most significant were weaknesses associated with the department's Centers for Medicare and Medicaid Services (CMS), formerly known as the Health Care Financing Administration, which, during fiscal year 2000, was responsible for processing more than \$200 billion in Medicare expenditures. CMS relies on extensive data processing operations at its central office to maintain administrative data (such as Medicare enrollment, eligibility, and paid claims data) and to process all payments for managed care. Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

To correct reported weaknesses, several agencies took significant steps to redesign and strengthen their information security programs. For example, the Environmental Protection Agency has moved aggressively to reduce

---

<sup>31</sup>U.S. General Accounting Office, *Information Security: Weak Controls Place Interior's Financial and Other Data at Risk*; [GAO-01-615](#) (Washington, D.C.: July 3, 2001).

<sup>32</sup>U.S. General Accounting Office, *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program*; [GAO-01-307](#) (Washington, D.C.: Mar. 30, 2001).

<sup>33</sup>Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000, A-17-00-00014, Feb. 26, 2001.

---

## Agencies' GISRA Results Also Highlight Weaknesses

the exposure of its systems and data and to correct weaknesses we identified in February 2000.<sup>34</sup> While we have not tested their effectiveness, these actions show that the agency is taking a comprehensive and systematic approach that should help ensure that its efforts are effective.

As required by GISRA, agencies reviewed their information security programs, reported the results of these reviews and the IGs' independent evaluations to OMB, and developed plans to correct identified weaknesses. These reviews and evaluations showed that agencies have not established information security programs consistent with GISRA requirements and that significant weaknesses exist. Although agency actions are now underway to strengthen information security and implement these requirements, significant improvement will require sustained management attention and OMB and congressional oversight.

In its fiscal year 2001 report to Congress on GISRA, OMB notes that although examples of good security exist in many agencies, and others are working very hard to improve their performance, many agencies have significant deficiencies in every important area of security.<sup>35</sup> In particular, the report highlights six common security weaknesses: (1) a lack of senior management attention to information security; (2) inadequate accountability for job and program performance related to information technology security; (3) limited security training for general users, information technology professionals, and security professionals; (4) inadequate integration of security into the capital planning and investment control process; (5) poor security for contractor-provided services; and (6) limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

In general, our analyses of the results of agencies' GISRA reviews and evaluations also showed that agencies are making progress in addressing information security, but that none of the agencies had fully implemented the information security requirements of GISRA and all continue to have significant weaknesses. In particular, our review of 24 of the largest

---

<sup>34</sup>U.S. General Accounting Office, *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk*; [GAO/AIMD-00-215](#) (Washington, D.C.: July 6, 2000).

<sup>35</sup>Office of Management and Budget, *FY 2001 Report to Congress on Federal Government Information Security Reform* (February, 2002).

---

federal agencies showed that agencies had not fully implemented requirements to:

- conduct risk assessments for all their systems;
- establish information security policies and procedures that are commensurate with risk and that comprehensively address the other reform provisions;
- provide adequate computer security training to their employees including contractor staff;
- test and evaluate controls as part of their management assessments;
- implement documented incident handling procedures agencywide;
- identify and prioritize their critical operations and assets, and determine the priority for restoring these assets should a disruption in critical operations occur; or
- have a process to ensure the security of services provided by a contractor or another agency.

Improvement Efforts are Underway, but Challenges to Federal Information Security Remain

Information security improvement efforts have been undertaken in the past few years both at an agency and governmentwide level. However, given recent events and reports that critical operations and assets continue to be highly vulnerable to computer-based attacks, the government still faces a challenge in ensuring that risks from cyber threats are appropriately addressed. Accordingly, it is important that federal information security efforts be guided by a comprehensive strategy for improvement.

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security. This strategy should also consider other organizations with information security responsibilities, including OMB, which oversees and coordinates federal agency security, and interagency bodies like the CIO Council, which are attempting to coordinate agency initiatives. It should also describe how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals.

Second, more specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which to enforce these controls. In theory, this discretion is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence,

---

one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.<sup>36</sup> In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. Implementing such standards for federal agencies would require developing a single set of information classification categories for use by all agencies to define the criticality and sensitivity of the various types of information they maintain. It would also necessitate establishing minimum mandatory requirements for protecting information in each classification category.

Third, ensuring effective implementation of agency information security and critical infrastructure protection plans will require active monitoring by the agencies to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required by GISRA, would allow for more meaningful performance measurement. In addition, the annual evaluation, reporting, and monitoring process established through these provisions, is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective. Moreover, with GISRA expiring on November 29, 2002, we believe that continued authorization of information security legislation is essential to improving federal information security.

Fourth, the Congress and the executive branch can use audit results to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by the OMB and congressional efforts to oversee the Year 2000 computer challenge.

Fifth, agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems.

---

<sup>36</sup>U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*; [GAO/AIMD-98-68](#) (Washington, D.C.: May 1998).

---

Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. Highlighted during the Year 2000 challenge, the availability of adequate technical and audit expertise is a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their information security and infrastructure protection activities. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on information security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk management process.

Seventh, expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. As stated by the director of the CERT® Coordination Center in congressional testimony last September, "It is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches." In addition, in its December 2001 third annual report, the Gilmore Commission recommended that the Office of Homeland Security develop and implement a comprehensive plan for research, development, test, and evaluation to enhance cyber security.<sup>37</sup>

---

In conclusion, consolidating the six federal CIP-focused organizations into a single division within the proposed Department of Homeland Security, if properly organized and implemented, could minimize duplication and allow for closer coordination of national CIP approach, especially in the areas of outreach and education, the identification of critical assets, and incident reporting, analysis, and warning. However, prior GAO work has identified and made recommendations concerning several critical infrastructure protection challenges that need to be addressed. The new

---

<sup>37</sup>*Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Dec. 15, 2001).

---

department should be viewed as a catalyst for addressing these recommendations, which include:

- completing a comprehensive and coordinated CIP strategy to include both cyber and physical aspects,
- improving analytical and warning capabilities,
- improving information sharing both within the federal government and between the federal government and the private sector and state and local governments.
- addressing pervasive weaknesses in federal information security.

Mr. Chairman, this concludes my written testimony. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by e-mail at [daceyr@gao.gov](mailto:daceyr@gao.gov).

---

# Appendix: Organizations Proposed to Be Moved to the Information Analysis and Infrastructure Protection Division

---

Below is a description of the current roles and responsibilities for the six federal organizations that are proposed to be moved to the new division.

---

## Critical Infrastructure Assurance Office

As established under PDD 63, the Critical Infrastructure Assurance Office (CIAO) performs a variety of CIP functions in three major areas: (1) educating the private sector on the importance of CIP, (2) preparing the national CIP strategy, and (3) assisting federal civilian agencies and departments in determining their dependencies on critical infrastructures.

First, the CIAO works to educate industry representatives that critical infrastructure assurance must be addressed through corporate risk management activities. Its efforts focus on the critical infrastructure industries (e.g., information and communications, banking and finance, transportation, energy, and water supply), particularly the corporate boards and chief executive officers who are responsible for setting policy and allocating resources for risk management. In addition to infrastructure owners and operators, this office's awareness and outreach efforts also target members of the audit, insurance, and investment communities. CIAO's goal is to educate these groups on the importance of assuring effective corporate operations, accountability, and information security.

Second, the CIAO is tasked with working with government and industry to prepare the national strategy for CIP, which is due for completion in 2002. This strategy will serve as the basis for CIP legislative and public policy reforms, where needed. The development of the national strategy for CIP is to also serve as part of an ongoing process in which government and industry will continuously modify and refine their efforts to ensure the safety of critical information systems.

Third, the CIAO is responsible for assisting civilian federal agencies and departments in analyzing their dependencies on critical infrastructures. This mission is conducted under Project Matrix, a program designed to identify and characterize the assets and associated infrastructure dependencies and interdependencies that the government requires to fulfill its most critical responsibilities. Project Matrix involves a three-step process in which each federal civilian agency identifies (1) its critical assets; (2) other federal government assets, systems, and networks on which those critical assets depend to operate; and (3) all associated dependencies on privately owned and operated critical infrastructures.

Additional cyber CIP duties were added to CIAO under Executive Order 13231, including having its director serve as a member of and advisor to

---

the President's Critical Infrastructure Protection Board. The CIAO is also to support the activities of the National Infrastructure Advisory Council, a group of 30 representatives from private industry and state and local government that will advise the President on matters relating to cybersecurity and CIP. In addition, the CIAO is expected to administer a Homeland Security Information Technology and Evaluation Program to study and develop methods to improve information sharing among federal agencies and state and local governments.

---

## Federal Computer Incident Response Center

The Federal Computer Incident Response Center (FedCIRC) is the focal point for dealing with computer-related incidents affecting federal civilian agencies. Originally established in 1996 by the National Institute of Standards and Technology, the center has been administered by the General Services Administration since October 1998.

FedCIRC's primary purposes are to provide a means for federal civilian agencies to work together to handle security incidents, share related information, and solve common security problems. In this regard, FedCIRC

- provides federal civilian agencies with technical information, tools, methods, assistance, and guidance;
  - provides coordination and analytical support;
  - encourages development of quality security products and services through collaborative relationships with federal agencies, academia, and private industry;
  - promotes incident response and handling procedural awareness within the federal government;
  - fosters cooperation among federal agencies for effectively preventing, detecting, handling, and recovering from computer security incidents;
  - communicates alert and advisory information regarding potential threats and emerging incident situations; and
  - augments the incident response capabilities of federal agencies.
- In accomplishing these efforts, FedCIRC draws on expertise from the Department of Defense, the intelligence community, academia, and federal civilian agencies. In addition, FedCIRC collaborates with the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center in planning for and dealing with criminal activities that pose a threat to the critical information infrastructure.

---

## National Communications System

Created by Executive Order 12472, the National Communications System's (NCS's) CIP mission is to assure the reliability and availability of national security and emergency preparedness (NS/EP) telecommunications. Its mission includes, but it is not necessarily limited to, responsibility for (1) assuring the government's ability to receive priority services for NS/EP purposes in current and future telecommunications networks by conducting research and development and participating in national and international standards bodies and (2) operationally coordinating with industry for protecting and restoring NS/EP services in an all-hazards environment. NCS's mission is externally focused on the reliability and availability of the public telecommunications network. This mission is carried out within government through the NS/EP Coordinating Committee, with industry on a policy level in coordination with the National Security Telecommunications Advisory Committee (NSTAC), and operationally through the National Coordinating Center for Telecommunications and through its participation in national and international standards bodies. Furthermore, in January 2000, National Coordinating Center was designated an ISAC for telecommunications under the provisions of PDD 63.

NCS reports to the Executive Office of the President–National Security Council for policy, to the Office of Science Technology and Policy for operations, and to OMB for budget through the Secretary of Defense, who is the Executive Agent for NCS. NCS's NS/EP Coordinating Committee is a standing committee under the President's Critical Infrastructure Protection Board. Externally, NCS coordinates with the Office of Cyberspace Security; CIAO; the National Telecommunications and Information Administration; the NIPC; GSA's FedCIRC; the Department of Energy (DOE) (including several of the laboratories); the Department of Transportation (DOT), industry members of the National Coordinating Center for Telecommunications; ISACs; and numerous DOD organizations.

---

## National Infrastructure Protection Center

NIPC, a multiagency organization located within the FBI, detects, analyzes, and warns of cyberthreats to and/or attacks on the infrastructure, should they occur. NIPC's mission is based on authorities given in Executive Order 13231 and PDD 63. In addition, the center is responsible for accomplishing the FBI's role as lead agency for sector liaison for the Emergency Law Enforcement Services Sector. As a sector liaison, NIPC provides law enforcement response for cyberthreats and crimes involving or affecting critical infrastructures. NIPC also facilitates and coordinates the federal government's response to cyber incidents, mitigating attacks, and investigating threats, as well as monitoring

---

reconstitution efforts. NIPC regularly coordinates with federal, state, local, and law enforcement and intelligence agencies resident in the NIPC: FBI, DOD, the Central Intelligence Agency, the National Security Agency (NSA), the United States Secret Service, Commerce, DOT, DOE, and other federal agencies on the President's Critical Infrastructure Protection Board, as well as Canada and Great Britain.

In addition, NIPC runs the National InfraGard program, which is a cooperative undertaking between the federal government and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of critical infrastructures. InfraGard's goal is to enable the flow of information so that the owners and operators of infrastructure assets, the majority of which are from the private sector, can better protect themselves and so that the U.S. government can better discharge its law enforcement and national security responsibilities. InfraGard provides members a forum for education and training on infrastructure vulnerabilities and protection measures and with threat advisories, alerts, and warnings.

NIPC comprises three sections: (1) the Computer Investigations and Operations Section, which is the operational and response arm and is responsible for designing, developing, implementing, and managing automated tools NIPC uses to collect, analyze, share, and distribute information; and coordinating computer investigations conducted by the FBI's 56 field offices and approximately 400 sublocations throughout the country; (2) the Analysis and Warning Section, which is the indication and warning arm, which provides support during computer intrusion investigations; and (3) the Training, Outreach, and Strategy Section, which provides outreach to the private sector and to local law enforcement, and training and exercise programs for cyber and infrastructure protection investigators within the FBI and other agencies.

---

## National Infrastructure Simulation and Analysis Center

The National Infrastructure Simulation and Analysis Center (NISAC) exists as a partnership between the Defense Threat Reduction Agency and the Los Alamos and Sandia national laboratories. Its mission is to improve the robustness of the nation's critical infrastructures by providing an advanced modeling and simulation capability that will enable an understanding of how the infrastructure operates; help identify vulnerabilities; determine the consequences of infrastructure outages; and optimize protection and mitigation strategies. NISAC's objectives are to

---

leverage the existing capabilities of the NISAC partners to provide leadership in critical infrastructure interdependencies modeling, simulation, and analysis;

- establish a virtual capability that will provide a portal for nation-wide remote access and communications to infrastructure-related modeling, simulation, and analysis capabilities;
- move toward a predictive capability that uses science-based tools to understand the expected performance of interrelated infrastructures under various conditions;
- provide simulation and analysis capabilities to a wide range of users that will enhance the understanding of vulnerabilities of the national infrastructures and establish priorities and potential mitigation strategies for protecting the infrastructures;
- provide decision-makers the ability to assess policy and investment options that address critical infrastructure needs – near and long term;
- provide education and training to public and private decision makers on how to cope effectively with crisis events; and
- provide an integrating function that includes interdependencies; bring disparate users and information providers and individual infrastructure sector leaders together.

---

## National Institute of Standards and Technology—Computer Security Division

Under the Computer Security Act of 1987, NIST's Computer Security Division of the Information Technology Laboratory develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Specifically, the Computer Security Division's mission is to improve information systems security by

- raising awareness of IT risks, vulnerabilities, and protection requirements, particularly for new and emerging technologies;
- researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive federal systems;
- developing standards, metrics, tests, and validation programs to
  - promote, measure, and validate security in systems and services
  - educate consumers and
  - establish minimum security requirements for federal systems; and
- developing guidance to increase secure IT planning, implementation, management, and operation.

Further, the division's functions are focused on five areas:

- 
- cryptographic standards and applications,
  - security research and emerging technologies,
  - security management and guidance,
  - security testing, and
  - outreach, awareness, and education.